your Gateway Windows network

# installationguide

802.11b wireless series | Router model WBR-100

Installing          Configuring          **Gateway**®

# Contents

# Introduction

This chapter introduces the Gateway Wireless 802.11b access point router.

Read this chapter to learn about:

- Product features
- Safety
- Package contents
- Connectors and LEDs
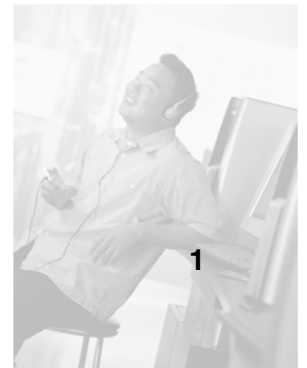
# Features

Your Gateway Wireless Router features:

■ Compact, modern design

■ High speed (11 Mbps in the 2.4 GHz band - 802.11b)

■ Remote administration and firmware upgrades through the Internet

■ DHCP service to your network

■ Sophisticated security features, including up to 128-Bit WEP encryption, Web and port filtering, WAN request blocking and DMZ hosting

■ Virtual Private Networking (VPN) over the Internet (with IPSec, L2TP, and PPTP pass-through)

# Important safeguards

**Warning**

Do not attempt to remove the cover. There are no user-serviceable parts inside. Removing the cover voids the warranty.

Have your wireless router repaired by qualified service personnel only.

# Precautions

■ Do not place your wireless router in direct sunlight or near a heat source, as this may damage the housing or electronic components of the device.

■ Do not open or try to repair the device yourself.

■ Do not place your wireless router in a damp or excessively humid location, such as a bathroom.

■ To avoid possible electrical damage due to power surges, use a shielded, anti-surge plug-strip.

■ To avoid possible damage due to lightning, turn off and unplug the router during electrical storms.

# Package contents

Along with your wireless router, the package also contains the following items:

**AC Adapter**

**Ethernet cable**

**User's guide**

# Parts and accessories

The following additional parts and accessories may be helpful in setting up your wireless network:

■ Wireless Network Controller cards (for computers or notebooks)

■ RJ-45 (Cat-5) network cables (various lengths)

Contact Gateway for information on ordering these and other accessories.

# Front



| LED | Description |
|-----|-------------|
| Power | **Off** - The router is turned off |
|  | **On (green)** - Power on |
|  | **Flashing (green)** - After a firmware upgrade |
| Wireless | **On (green)** - The wireless mode is on |
| WAN | **Flashing (green)** - Activity on the WAN connection |

| LED | Description |
| --- | --- |
| LAN 4 - 1 | **Off** - The connection does not have an Ethernet link |
| | **On (green)** - Ethernet link detected on indicated connection |
| | **Flashing (green)** - Data traffic on indicated connection |

# Back

Antenna

Power connection     WAN Port

LAN Ports          Reset switch
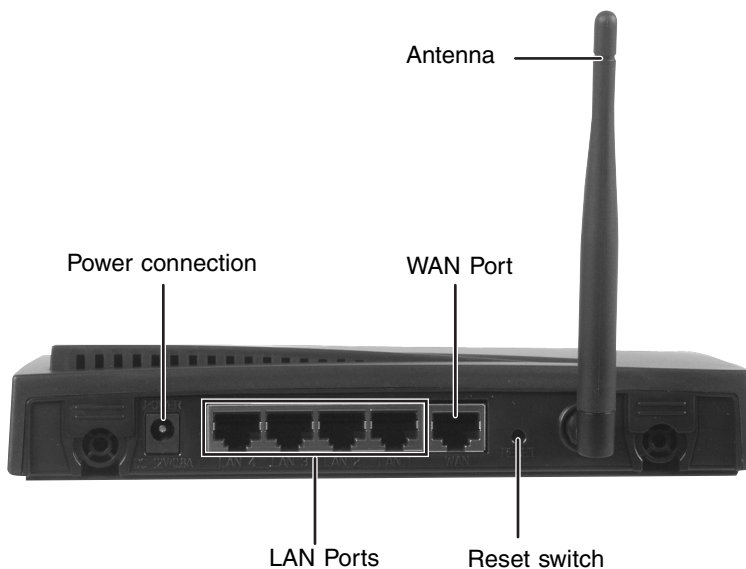
| Connector/control | Description |
|---|---|
| Power connection | Plug the AC adapter into this connection and plug the power cord into the AC adapter. Use only the AC adapter and power cord that came with the wireless router. Use of any other AC adapter or power cord may damage your router and void the warranty. |
| Reset switch | Press the reset button to return all configuration settings to the default settings. |
| WAN port | Connect the DSL or cable modem to this RJ-45 Ethernet port. |
| LAN ports | Connect a computer, hub, or switch to these RJ-45 Ethernet ports. |

# 2
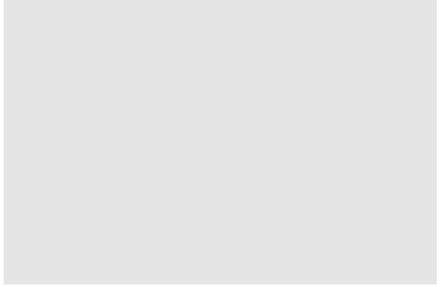
# Initial setup

Read this chapter to learn how to:

- ■ Make connections
- ■ Configure the computers
- ■ Contact and configure the router

# Making connections

## Preparation

If you intend to use the router to connect your network to the Internet, you need a broadband Internet connection (DSL or cable). You also need the following information and equipment:

- A host computer (initially connected to router to enter configuration information) that has a network interface card.

- An RJ-45 Ethernet cable (Cat-5 or better)
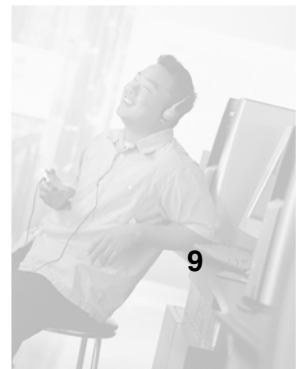
- A DSL or cable modem (purchased or provided by your ISP)

- Host computer's IP address (assigned by your ISP, if a static IP address is required)

- Subnet mask (assigned by your ISP, if a static IP address is required)

- Default gateway (assigned by your ISP, if a static IP address is required)

- Primary DNS IP address (assigned by your ISP, if a static IP address is required)

- Host computer's name and workgroup (available through the Windows Control Panel under System information)

## Connecting the hardware

### To connect the hardware:

**1** Turn off and unplug the host computer, the DSL or cable modem, and the router.

**2** Using an RJ-45 Ethernet cable (Cat-5 or better), connect the Ethernet port of the host computer to the LAN 1 connection on the back of the router.

**3** Using an RJ-45 Ethernet cable (Cat-5 or better), connect the Ethernet port on your DSL or cable modem to the WAN connection on the back of router.

| **Warning** | Use only the AC adapter and power cord provided with the router. Use of any other adapter or power cord your router and void your warranty |
| --- | --- |

**4** Plug the AC adapter into the power cord, then plug the power cord into an electrical outlet. Connect the other end of the adapter to the power connector on the back of the router. (see the illustration on "Back" on page 8)

- The green Power LED turns on
- The green Wireless LED turns on

**5** Turn on the DSL or cable modem. Check the LEDs on the modem to make sure that the modem is connected and operating normally. The WAN LED on the router lights when the modem is connected correctly to the router.

**6** Turn on the host computer. The LAN LED corresponding to the RJ-45 jack used for the LAN connection on the router lights when the computer is connected correctly to the router.

# Configuring the computers

Now that you have the hardware connected, you need to configure the computers you want to include in your network to let them obtain an IP address automatically. An IP address lets the computers communicate with and operate on your new network. Use the configuration procedure specific to your computer's operating system:

## To configure computers using Windows XP:

1 Click **Start**, then click **Control Panel**. The *Control Panel* window opens. If your Control Panel is in Category View, click **Network and Internet Connections**.

2 Click/Double-click **Network Connections**. The *Network Connections* window opens.

3 Double-click the **Local Area Connection** icon for your network interface card. If you see more than one, double-click the one that connects to your local network. The *Local Area Connection Status* dialog box opens. Click **Properties**.

4 In the **Components checked are used by this connection** list, click **Internet Protocol (TCP/IP)**, then click **Properties**.

5 Check **Obtain an IP address automatically**, and make sure that **Obtain DNS server address automatically** is selected.

6 Click **OK** to accept the settings.

7 Click **OK** again to exit.

8 Repeat Step 1 through Step 7 for each computer on your network running Windows XP.

## To configure computers using Windows 2000:

1 Click **Start**, **Settings**, then click **Control Panel**.

2 Double-click the **Network and Dial-up Connections** icon to open the *Network* dialog box.

**3** Double-click the **Local Area Connection** icon for your network interface card. If you see more than one icon, select the one that connects to your local network. The *Local Area Connection Status* dialog box opens. Click **Properties**.

**4** In the **Components checked are used by this connection** list, click **Internet Protocol (TCP/IP)**, then click **Properties**.

**5** Check **Obtain an IP address automatically**, and make sure that **Obtain DNS server address automatically** is selected.

**6** Click **OK** to accept the settings.

**7** Click **OK** again to exit.

**8** Repeat Step 1 through Step 7 for each computer on your network running Windows 2000.

## To configure computers using Windows 98SE or Me:

**1** Click **Start**, **Settings**, then click **Control Panel**.

**2** Double-click the **Network** icon to open the *Network* dialog box.

**3** Click the **Configuration** tab, click the TCP/IP protocol for your network interface card, then click **Properties**. If you do not see TCP/IP, you need to install the TCP/IP protocol. See the documentation that came with your network interface card for information on installing the TCP/IP protocol)

**4** Check to select the **Obtain an IP address automatically** check box, then click the **Gateway** tab and make sure that the **Installed gateways** box is not selected.

**5** Click **OK** to accept the settings.

**6** Click **OK** again to exit. Follow any on-screen instructions.

**7** Reboot your system.

**8** Repeat Step 1through Step 7 for each computer on your network running Windows 98SE or Me.

# Contacting and configuring the router

Now that all the hardware connections have been made, you must configure the router must to operate on your network and to connect to the Internet through an ISP.

Initial configurations vary somewhat, depending on your ISP. Contact your ISP before you configure your router, and determine the following:

- If your ISP assigns a static IP address or provides one automatically (DHCP) each time you connect to the ISP

- For an automatic IP address, the **Host Name** (if required) and the **Domain Name** (if required)

- For a static IP address, the IP address, subnet mask, default gateway, and DNS address (at least one)

- If you are connected with a DSL modem using Point to Point Protocol over Ethernet (PPPoE), or if your ISP requires a **user name** and **password**, the user name and password you need to use

- If your ISP uses RAS (Singapore) or PPTP (Europe), instructions for setting up.

## Contacting the router

### To contact the router:
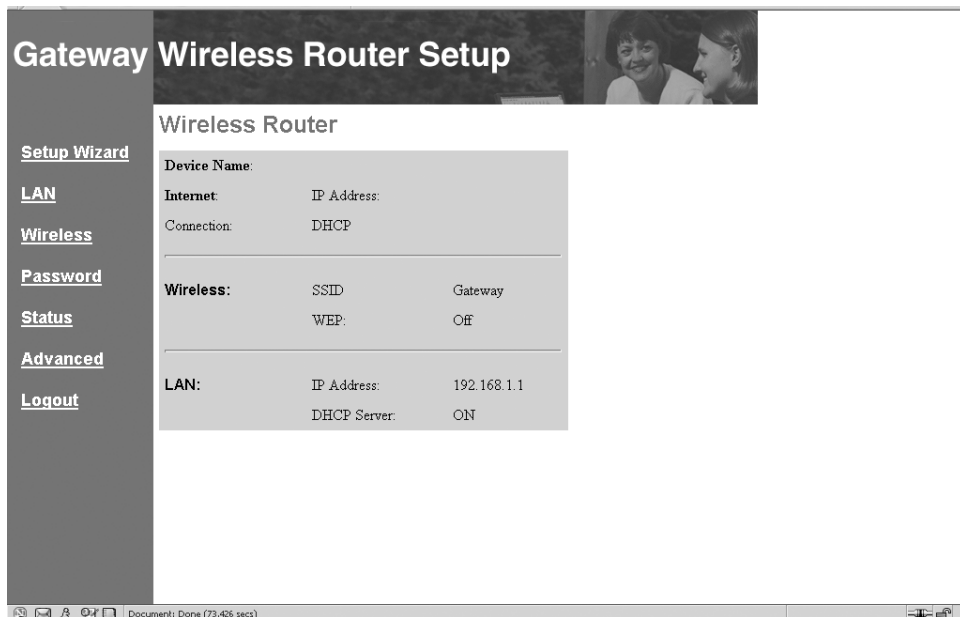
**1** Launch your Web browser on the host computer.

**2** In the address box, type **192.168.1.1**, then press **ENTER**. A message tells you to enter a User name and Password.



**3** When a message tells you to enter a User name and Password, type **admin** in both boxes (the default), then click **OK**. The *Setup* page opens.



**4** Go to "Configuring the router" on page 16.

# Configuring the router

Use the router Setup Wizard to do the initial configuration of the router. The Setup Wizard steps you through the process by asking you a series of questions. If you cannot answer some of the questions, contact your ISP for additional information. After the Setup Wizard has finished, the initial configuration of your router should be complete.
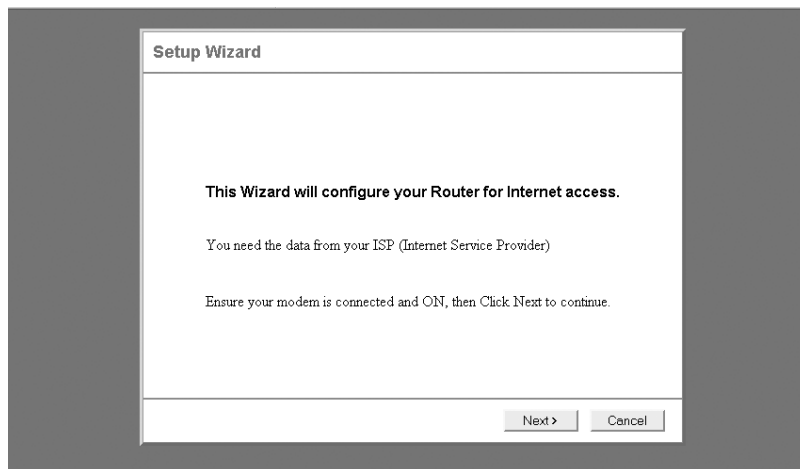
For help or additional information on any of the configuration windows described here, click items with **bold blue lettering** or the **Help** button at the bottom of the window.

## The Setup Wizard

▶ **To configure the router:**

**1** After accessing the *Setup* page (see "Contacting the router" on page 14), click **Setup Wizard** in the left column. The *Setup Wizard* window opens. Click **Next** to continue.

```
  Setup Wizard
  ─────────────────────────────────────────────

       This Wizard will configure your Router for Internet access.

       You need the data from your ISP (Internet Service Provider)

       Ensure your modem is connected and ON, then Click Next to continue.



                                              [ Next > ]   [ Cancel ]
```

**2** In the *Setup Wizard - Internet Access* window, click the type of Internet access you have. If you are not sure what kind of service you have, look on your modem (it may say Cable Modem or DSL Modem) or contact your ISP for the information. When you have made your selection, click **Next** to continue.
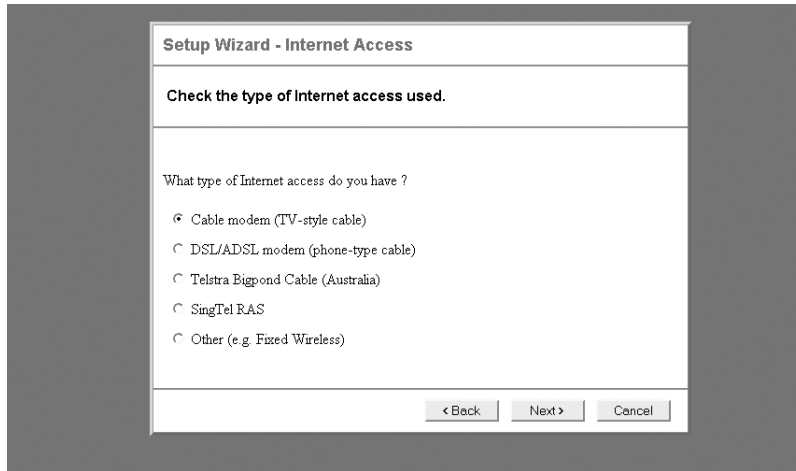


**3** If you selected **Cable Modem**, type the **Hostname** and **Domain Name** (if required by your ISP), and the **Login method**. Do not change the default MAC (physical) Address unless your ISP recorded your computer's hardware address and requires it for your Internet connection. If this is the case, click **Clone MAC Address** to have your computer's MAC address copied to the router. Click **Next** to continue.

Indicate how the **IP Address** is assigned by your ISP. If they assign one automatically each time you connect, select **Dynamic**. If they specify an IP address that does not change, select **Static** and type the IP Address, the subnet mask, the default gateway, and the DNS. Click **Next** to finish.

**4** If you selected **DSL/ADSL Modem,** select the type of **Login** (if any) used for Internet access. Click **Next** to continue.

- ■ **PPPoE** - Type the **User Name** and **Password** provided by your ISP. Also, indicate if you connect automatically, and the interval that elapses before you are automatically disconnected. Click **Next** to continue.

    - OR -

- ■ **PPTP** (Europe only) - Enter the **PPTP Server IP Address**, the **User Name** and **Password** provided by your ISP. Also, indicate if you connect automatically, and the interval that elapses before you are automatically disconnected. Click **Next** to continue.

    - THEN -

- ■ Indicate how the **IP Address** is assigned by your ISP. If they assign one automatically each time you connect, select **Dynamic**. If they specify an IP address that does not change, select **Static** and type the IP address, the subnet mask, the default gateway, and the DNS. Click **Next** to finish.

**5** If you selected **Telstra Bigpond Cable (Australia)**:

- ■ Enter the **Server IP Address**, the **Login User Name** and **Login Password** provided by your ISP. Also, indicate if you connect automatically, and the interval that elapses before you are automatically disconnected. Click **Next** to continue.
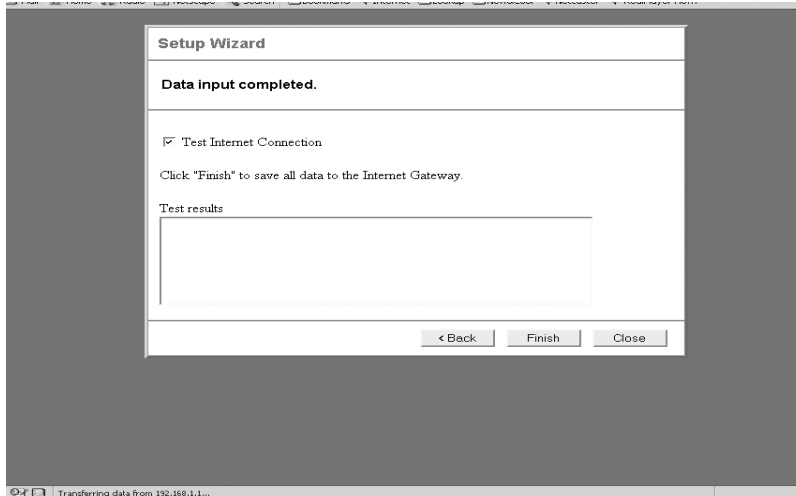
    - THEN -

- ■ Indicate how the **IP Address** is assigned by your ISP. If they assign one automatically each time you connect, select **Dynamic**. If they specify an IP address that does not change, select **Static** and type the IP Address, the subnet mask, the default gateway, and the DNS. Click **Next** to finish.

**6** If you selected **SingTel RAS**:

- ■ Type the **Login User Name** and **Login Password** provided by your ISP. Also, select the type of RAS Plan you have (512k or 256k Ethernet), then indicate if you connect automatically (as needed), or if your connection is always maintained. Click **Next** to finish.

**7** If you selected **Other (e.g., Fixed Wireless)**:

■ Indicate how the **IP Address** is assigned by your ISP. If they assign one automatically each time you connect, select **Dynamic**. If they specify an IP address that does not change, select **Static** and type the IP Address, the subnet mask, the default gateway, and the DNS. Click **Next** to finish.

**8** Click **Finish** to complete the initial router configuration. We suggest that you leave the check in the **Test Internet Connection** check box to have the connection tested automatically.

**Setup Wizard**

**Data input completed.**

☑ Test Internet Connection

Click "Finish" to save all data to the Internet Gateway.

Test results

< Back    Finish    Close

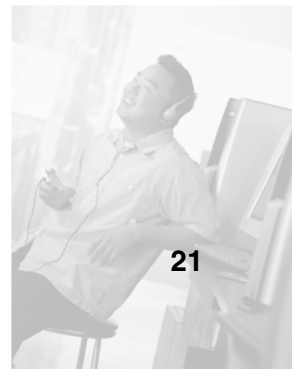Transferring data from 192.168.1.1...

# Routine Router Settings and Status

# 3

Read this chapter to learn how to:

- Set up LAN settings
- Set up wireless settings
- Reset the password
- Check router status
- Set up security for wireless operation
- Restore the router's default settings

# Using router settings and features

The router comes with pre-set settings that let it operate in most situations. You can make changes to these settings if you want to turn on additional features on your router or to make your router conform to your ISP's requirements for Internet access.

The Gateway Wireless Router Setup utility lets you turn many of the router's features on and off to customize your network.

## Configuring LAN settings

These settings configure the router for operation within your local area network. The LAN IP address is the address your computers see and the address they use to contact the router.

We recommend that you use the default values for IP address and subnet mask, unless the address is already being used in your LAN or your LAN is using a different address range.

### To configure the LAN settings:

**1** After accessing the *Setup* page (see "Contacting the router" on page 14), click **LAN** in the left column. The *LAN* window opens.

**2** If the IP address and subnet mask must be changed, type the new IP address and subnet mask in the boxes provided, otherwise leave the default settings.

**3** In the **DHCP Server** box, make sure that the check box is selected (default) if you want the router to provide DHCP service to your network (by assigning an IP address automatically to each computer on your network when they sign on). Click the box to remove the check only if you have another router or DHCP server on your network providing this service.

The **Start IP Address** is the first IP address assigned by the router. Subsequent IP addresses will increment by one until all addresses are assigned (up to the **Finish IP Address**). The first three fields are assigned by the router to match the router's IP address and function correctly in the LAN.

The **Finish IP Address** is the last IP address assigned by the router. It determines the maximum number of IP addresses that can be assigned by the router. The first three fields are assigned by the router to match the router's IP address and function correctly in the LAN.
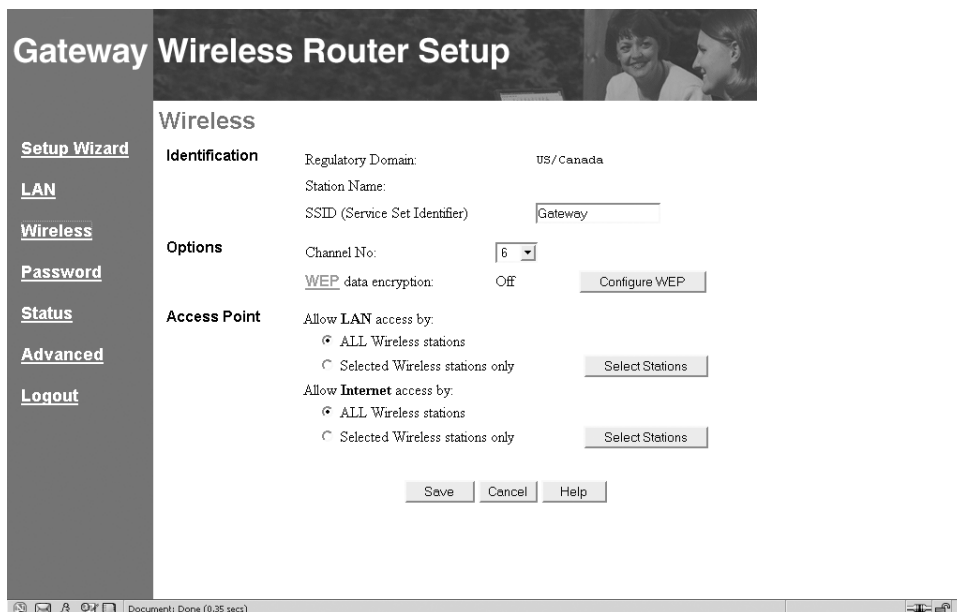
**4** Click **Save** to save your entries or **Cancel** to remove your changes and return to the default settings.

# Configuring wireless settings

▶ **To configure the wireless settings:**

**1** After accessing the *Setup* page (see "Contacting the router" on page 14), click **Wireless** in the left column. The *Wireless* window opens. In the Identification area, the **Regulatory Domain** and **Station Name** are automatically provided.

**Gateway Wireless Router Setup**

Wireless

| | | |
|---|---|---|
| **Setup Wizard** | **Identification** | Regulatory Domain:       US/Canada |
| **LAN** | | Station Name: |
| **Wireless** | | SSID (Service Set Identifier)    Gateway |
| **Password** | **Options** | Channel No:    6 ▾ |
| **Status** | | WEP data encryption:    Off    Configure WEP |
| **Advanced** | **Access Point** | Allow **LAN** access by: |
| **Logout** | | ○ ALL Wireless stations |
| | | ○ Selected Wireless stations only    Select Stations |
| | | Allow **Internet** access by: |
| | | ○ ALL Wireless stations |
| | | ○ Selected Wireless stations only    Select Stations |

Save    Cancel    Help

Document: Done (0.35 secs)

**2** Type the name of your wireless LAN in the **SSID (service set identifier)** box. This must be consistent for your entire local network. It is case sensitive and can be up to 32 alphanumeric characters in length.

| **Important** | The SSID must be exactly the same for all wireless stations on your entire local wireless network. Wireless stations with a different setting will be unable to communicate with the rest of the network. |
|---|---|

**3** In the Options section, click the arrow to open the **Channel** list, then click the channel number (1 - 11) you want. We recommend that you leave the default setting (6) unless another wireless network in your area is using that channel. Select an unused channel if that is the case.

**4** If you want to configure WEP (Wired Equivalent Privacy) security for your wireless network:

    **a** Click **Configure WEP.** The *Wireless - WEP Data Encryption* window opens.

| **Important** | WEP must be configured exactly the same for all wireless stations on your entire local wireless network. Wireless stations with different settings will be unable to communicate with the rest of the network. |
| --- | --- |



    **b** Click the arrow to open the **WEP Data Encryption** list, then click 64-bit or 128-bit encryption (Disable is the default). The higher level offers more security but may slow network speed.

    **c** Click the arrow to open the **Authentication Type** list, then click the type of authentication you want to use (Automatic is the default). If you select a different type of authentication, make sure that the rest of your network uses the same setting.

**d** In the **Key input** area, click the type of encryption key you want to use:

**Hex** (64 bit = 10 characters, or 128 bit = 26 characters)

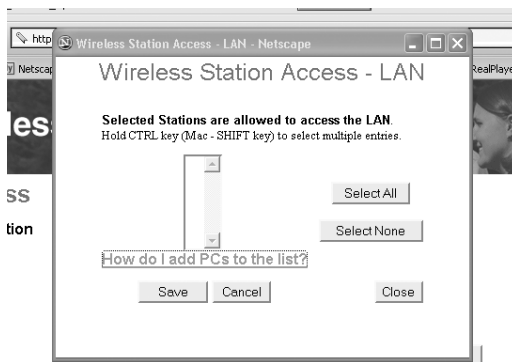**ASCII** (64 bit = 5 characters, or 128 bit = 13 characters).

**e** Select the **Default Key** to use on your wireless network, then type a key value in the field provided (see Step d).

- OR -

Select the **Default Key** to use on your wireless network, then type a Passphrase and click **Generate Keys** to have the router generate an encryption key, based on your selected parameters (see Step d).

**f** Click **Apply** to accept your changes or **Cancel** to remove your entries and return to default values, then click **Close** to return to the *Wireless* screen.

**5** In the Access Point section, under **Allow LAN access by,** click **ALL Wireless stations** or **Selected Wireless stations only**. If you clicked **Selected Wireless stations only**, click **Select Stations**.



The computers listed are current DHCP clients or have been added manually to the PC Database on the **Advanced** menu. If a DHCP client is not listed, restart the computer.

Select the computers you want to have access to your wireless network. To select multiple computers, hold down the CTRL key (Mac - SHIFT key) when you click computer names, or click **Select All** or **Select None**.

**6** Click **Apply** to accept your changes or **Cancel** to remove your entries and return to default values, then click **Close** to return to the *Wireless* screen.

**7** In the **Access Point** section, under **Allow Internet access by,** click **ALL Wireless stations** or **Selected Wireless stations only**. If you clicked **Selected Wireless stations only**, click **Select Stations**.

The computers listed are current DHCP clients or have been added manually to the PC Database on the **Advanced** menu. If a DHCP client is not listed, restart the computer.

Select the computers you want to have access to your wireless network. To select multiple computers, hold down the **CTRL** key (Mac - **SHIFT** key) when you click computer names, or click **Select All** or **Select None**.

**8** Click **Apply** to accept your changes or **Cancel** to remove your entries and return to default values, then click **Close** to return to the *Wireless* screen.

**9** Click **Save** to accept your Wireless changes or **Cancel** to remove your entries and return to default values.

# Changing the password

This screen allows you to change the router password from the default (admin) setting or from the current setting. You will be prompted for the password each time you attempt to open the Gateway Wireless Router Setup utility.

## To change the password:

**1** Click **Password** in the left column. The **Password** screen opens.

**2** In the **New Password** field, type the new password (up to 9 alphanumeric characters).

**3** In the **Verify Password** field, type the same password to confirm your change.

**4** Click **Save** to accept your Password change or **Cancel** to remove your entry and return to the default setting.
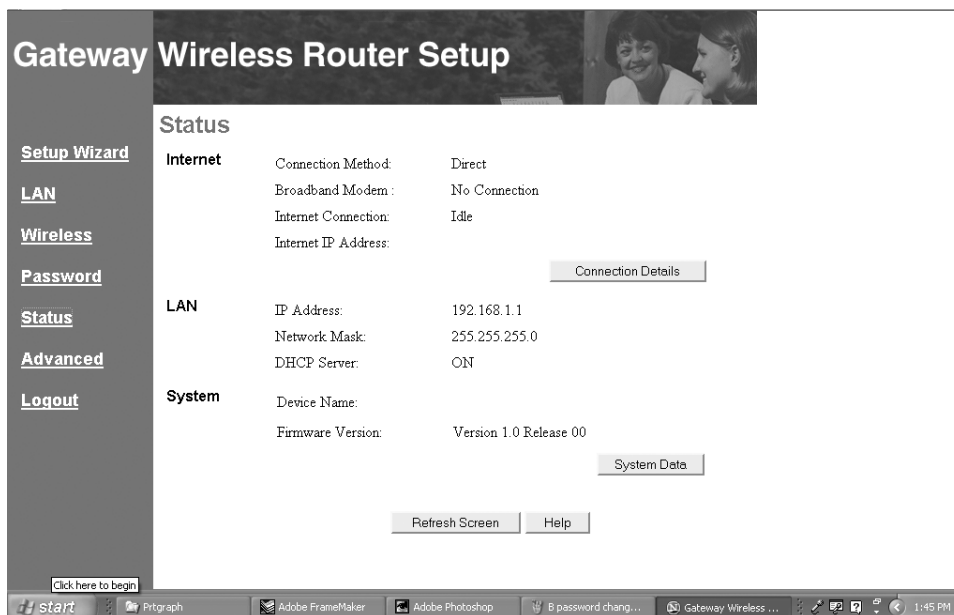
# Checking router status

The current settings and status of the router can be determined by accessing the *Status* screen. The information provided includes Internet, LAN, and System status/settings.
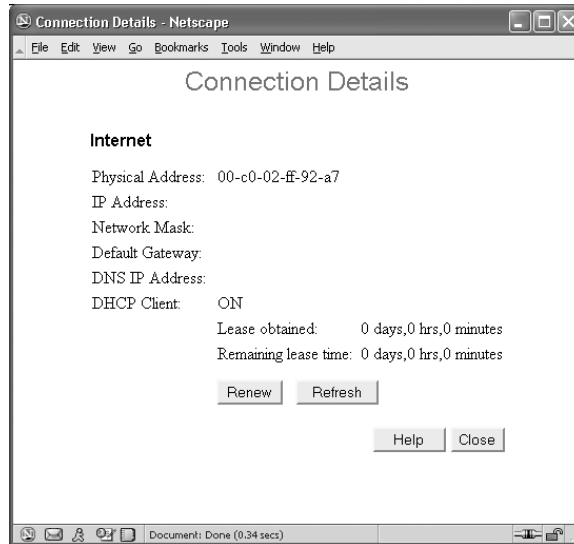
▶ **To review the router status:**

**1** Click **Status** in the left column. The *Status* window opens.

**2** For detailed information on the connection, click **Connection Details**. The *Connection Details* screen opens.

**3** Click **Release** if the wireless router is using a dynamic IP address assigned by your ISP's DHCP server. Release will release the IP address and break the connection.
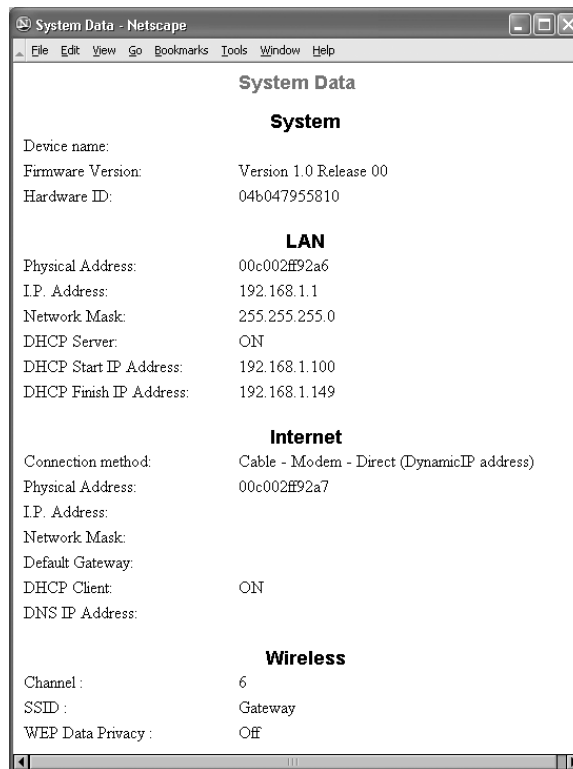
- OR -

Click **Renew** if the wireless router has not been assigned a dynamic IP address by your ISP's DHCP server. Renew will re-establish the connection with the ISP and obtain an IP address.

**4** Click **Refresh** to update the information on the screen.

**5** Click **Close** to exit the screen and return to the *Status* window.

**6** Click **System Data** to open a window that provides additional information about the current configuration and system status. Close the window when you want to return to the *Status* window.

```
System Data - Netscape                          [_][□][X]
 File  Edit  View  Go  Bookmarks  Tools  Window  Help

                        System Data
                          System
Device name:
Firmware Version:             Version 1.0 Release 00
Hardware ID:                  04b047955810

                            LAN
Physical Address:             00c002ff92a6
I.P. Address:                 192.168.1.1
Network Mask:                 255.255.255.0
DHCP Server:                  ON
DHCP Start IP Address:        192.168.1.100
DHCP Finish IP Address:       192.168.1.149

                         Internet
Connection method:            Cable - Modem - Direct (DynamicIP address)
Physical Address:             00c002ff92a7
I.P. Address:
Network Mask:
Default Gateway:
DHCP Client:                  ON
DNS IP Address:

                         Wireless
Channel :                     6
SSID :                        Gateway
WEP Data Privacy :            Off
```

**7** Click **Refresh Screen** to update the information on the screen.

■

# Setting up wireless operation

After the initial configuration is done, you can set up your network to work in wireless mode. To operate in wireless mode, each computer in your network must be equipped with a wireless network interface card and the SSID must be the same for each. For additional information on setting up your wireless network interface card, see the *Setting Up Your Wireless Windows Network* guide, or the documentation that accompanied your wireless network card.

## Configuring WEP security in Windows XP

Windows XP does not automatically configure the wireless adapter to use the encryption key generated when a WEP passphrase is entered. On computers running Windows XP, after the WEP encryption key has been generated (see "Configuring the router" on page 16), the key must be entered manually to let the system communicate with the router.

▶ **To manually enter the WEP encryption key in Windows XP:**

**1** Click **Start**, then click **Control Panel**. If your Control Panel is in Category View, click **Network and Internet Connections**.

**2** Click/Double-click **Network Connections**. The *Network* window opens.

**3** Double-click the **Wireless Network Connection** icon for your wireless network interface card. If more than one is shown, double-click the one that connects to your wireless network. When the *Wireless Network Connection Status* window opens, click **Properties**. The *Wireless Network Connection Properties* window opens.

**4** Click the **Wireless Networks** tab. If the correct wireless network (check the SSID) is shown in the **Preferred Networks** section, double-click it and continue to step 5, otherwise select it from the **Available Networks** section, then click **Configure**. The *Wireless Networks Properties* window opens.

**5** Click to select the **Data encryption (WEP enabled)** check box and click to clear the **The key is provided for me automatically** check box.

**6** In the **Network key** field, type the WEP encryption key that was generated when you configured the router.

| **Important** | The WEP encryption key must be typed exactly as generated. All 10 (64-bit encryption) or 26 (128-bit encryption) hexidecimal digits must be entered. |
| --- | --- |

**7** Make sure that the **Key format** field indicates hexidecimal digits and that the **Key length** field indicates the correct length key (10 or 26 digits).

**8** Click **OK** to accept the settings.

**9** Click **OK** again until you return to the Windows XP desktop.

**10** Close all applications and reboot the computer.

**11** Repeat Step 1 through Step 10 for each computer on your network running Windows XP.

# Returning the router settings to the default settings

The router comes with pre-set settings that let it operate in most situations. If you make changes to these settings and have difficulty contacting or operating the router, you can return the router settings to the default.

To return the router settings to the default, press the **Reset** switch on the back of the router for approximately 10 seconds. When you release the switch the Power and Wireless LEDs turn off, then turn back on. The router settings have been returned to the default values.

# Advanced Features and Configuration

# 4

Read this chapter to how to:

- Configure advanced Internet settings
- Configure access control settings
- Turn on remote management
- Set up a virtual server
- Use a dynamic DNS service
- Upgrade the firmware
- Use the PC Database
- Change router options
- Change security settings
- Change log settings
- Set the MAC address
- Configure routing
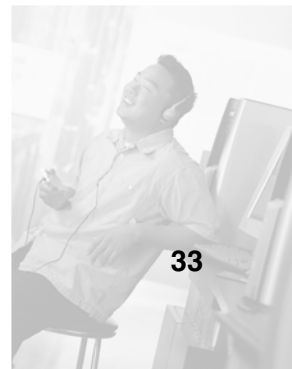
# Advanced features

Customizable settings are available under the *Advanced Features* heading for special applications, access control, remote management, establishing virtual servers, and upgrading the firmware on your router.

To access the *Advanced Features/Configuration* window, first open the Gateway Wireless Router Setup utility (see "Contacting the router" on page 14), then click **Advanced**. The *Advanced Features/Configuration* window opens.

| **Important** | We recommend that you do not change the default values found on these pages unless you are an advanced user with a complete understanding of the settings you are changing and the purpose for those changes. These settings determine the way your router sends and receives data and may limit or expand access to the router and your network. |
|---|---|

## Gateway Wireless Router Setup

### Advanced Features

Setup Wizard

LAN

Wireless

Password

Status

Advanced

Logout

| | |
|---|---|
| Advanced Internet | Special Applications, DMZ, URL Filter |
| Access Control | Define Internet access rights for PCs on your LAN. |
| Remote Management | Allow management of this device via the Internet. |
| Virtual Servers | Allow Internet users to access Servers on your LAN. |
| Dynamic DNS | Use with "Virtual Servers" to allow Internet users to connect to your Servers using a URL instead of an IP address. |
| Upgrade Firmware | The firmware can be upgraded using your Web Browser. |

### Advanced Configuration

| | |
|---|---|
| PC Database | View and modify the list of PCs. |
| Options | Backup DNS, TFTP firmware upgrade, UPnP. |
| Security | Firewall and other security-related settings. |
| Logs | Set system log options, E-mailing of logs, view all logs. |
| MAC Address | Set the MAC (hardware) address for the WAN (Internet) port. |
| Routing | Only required if your LAN has other Routers or Gateways. |

http://192.168.1.1/internet.htm

# Configuring advanced Internet settings

▶ **To configure the advanced Internet settings:**

**1** Begin on the *Advanced Features/Configuration* screen, then click **Advanced Internet** in the Advanced Features section. The *Advanced Internet* window opens.
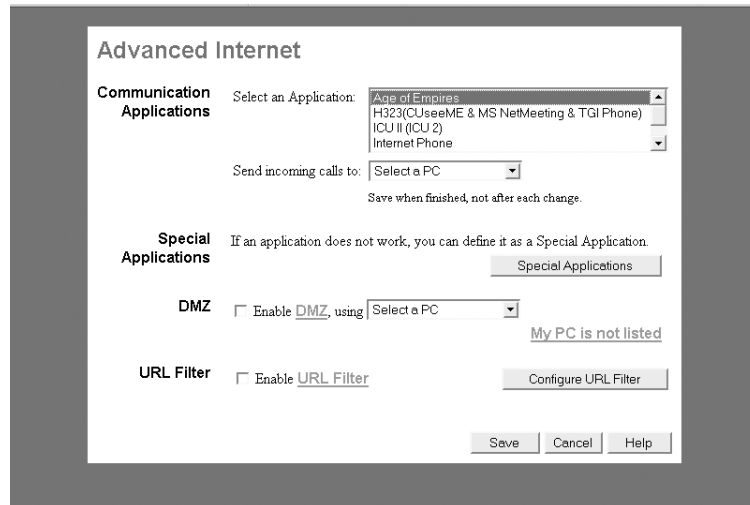


**2** In the Communication Applications area click an application in the **Select an Application** list. Included on the list are applications which may generate incoming connections to an unspecified address on your LAN.

Click the arrow to open the **Send incoming calls to** list, then click a destination computer for the application. You can also add computers manually by using the PC Database option under Advanced Configuration on the *Advanced Features/Configuration* window.

**3** If an application does not work through your LAN firewall, click **Special Applications**. The *Special Applications* window opens.
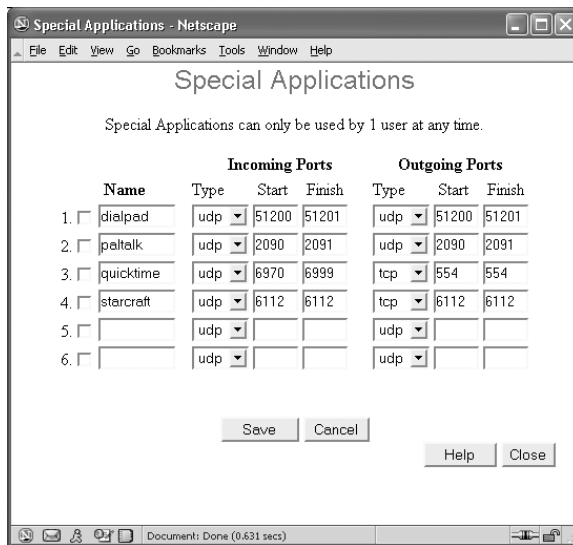


Click the check box next to a line, then type the name of the application in the **Name** box. Under Incoming Ports, click the arrow to open the **Type** list, click the protocol you use to receive data, then type the beginning and ending port numbers. Under Outgoing ports, click the arrow to open the **Type** list, click the protocol you use to send data, then type the beginning and ending port numbers.

Click **Save** to save your entries or **Cancel** to remove your entries, then click **Close** to exit the screen.

**4** In the DMZ (Demilitarized Zone) area, click the **Enable** check box to turn on DMZ hosting. DMZ hosting lets one computer on your network be exposed to the Internet for a specific purpose or application, such as Internet gaming or videoconferencing. If you choose to enable this feature, you must select a computer to host it and disable the DHCP function on the subject computer and assign it a static IP address (see "Setting a static IP address" on page 60).

**5** In the URL Filter area, click the **Enable** check box to turn on URL filtering, then click **Configure URL Filter**. The *URL Filter* screen opens.
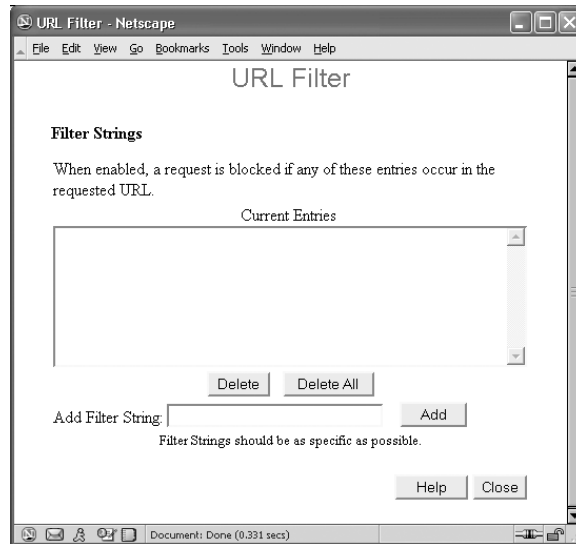


The **Current Entries** list shows the text strings currently being filtered (blocked) by the router. To add new strings of text (words or phrases) to be filtered, type the text in the **Add Filter String** box, then click **Add**. The new text string is moved to the **Current Entries** list.

To remove a text string from the **Current Entries** list, click the text, then click **Delete**. The entry is removed.

To remove all entries from the **Current Entries** list, click **Delete All**. All text strings are deleted.

**6** Click **Close** when you are finished. The *Advanced Internet* screen opens. Click **Save** to save your Advanced Internet entries or **Cancel** to return to the default settings. Close the window to return to the *Advanced Features/Configuration* window.
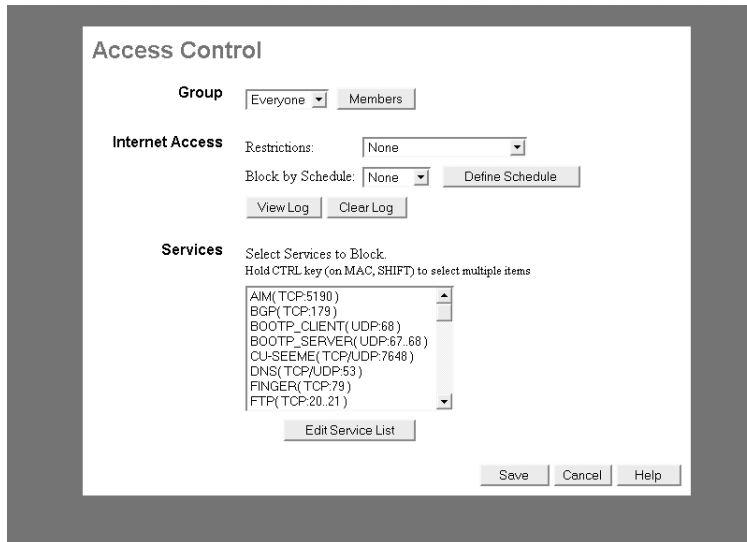
# Configuring access control settings

**To configure the Access Control settings:**

**1** Click **Access Control** in the Advanced Features section. The *Access Control* window opens.



**2** Click the arrow to open the **Group** list, then click the group whose access you want to control.

Click **Members** to open the *Group Members* screen, which shows a list of Members (by IP address) of the selected group and a list of Other computers (all other non-member computers).

To add computers to the group, click **Add**. To delete a computer from the group, click **Del**.

Click **Close** when you are finished viewing and editing the list. The *Access Control* screen opens.

**3** In the Internet Access section, click the arrow to open the **Restriction** list, then click one of the following:

- **None** for no blocking (lease restriction).

- **Block selected Services** for selective blocking (moderate restriction).

- **Block all Internet access** for maximum blocking (maximum restriction).

Click the arrow to open the **Block by Schedule** list, then click one of the following:

- **None** (for no scheduled blocking)

- **Default** (for scheduled blocking). If you select **Default**, click **Define Schedule** to set up a schedule. The *Default Schedule* screen opens.



Enter the **Start** and **Finish** times for the periods (Sessions) during which access will be blocked (at the level previously established). Do this for every day of the week that you want to block access. You can also choose to block access for two different periods (Sessions) during each day (for example, prior to 8:00 am and after 4:30 pm).

Click **Save** to save your schedule entries or **Cancel** to remove your entries, then click **Close** to return to the *Access Control* screen.

**4** Click **View Log** to see a log of blocked attempts to access the Internet. Click **Clear Log** to remove existing log entries and restart the log.

**5** In the Services section, click the services you want to block in the **Select Services to Block** list. To edit the list of services available to block, click **Edit Service List**. The *Services* screen opens.
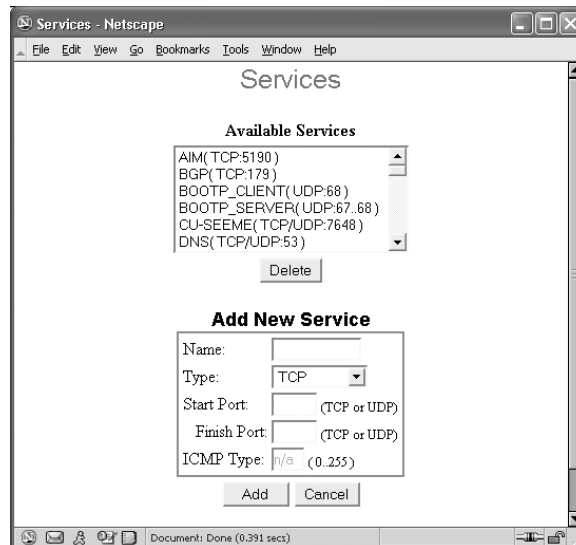


To delete a service from the **Available Services** list, click the service and click **Delete**.

To add services to the list, in the **Add New Service** box, type the name of the service in the **Name** box. Click the arrow to open the **Type** list, then click the protocol used by the service. Type the beginning and ending ports the service uses in the **Start Port** and **Finish Port** boxes. If you selected **ICMP** as the protocol, type the ICMP type instead of beginning and ending ports.

Click **Add** to add the new service to the **Available Services** list, or **Cancel** to remove your entry. Click **Close** to return to the *Access Control* screen.
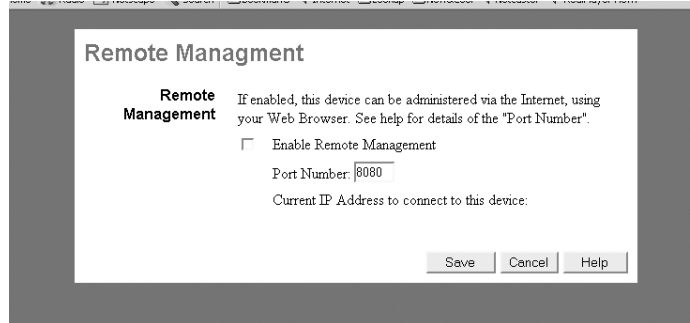
**6** Click **Save** to save your Access Control entries or **Cancel** to remove your entries. Close the window to return to the *Advanced Features/Configuration* window.

# Turning on remote management

▶ **To turn on remote management:**

**1** Click **Remote Management** in the Advanced Features section. The *Remote Management* window opens.

**Remote Managment**

Remote Management If enabled, this device can be administered via the Internet, using your Web Browser. See help for details of the "Port Number".

☐ Enable Remote Management

Port Number: 8080

Current IP Address to connect to this device:

Save | Cancel | Help

**2** To enable remote control of the router through, click to select the **Enable Remote Management** check box.

**3** Type the port number (between 1024 and 65535) by which the router will be remotely accessed in the **Port Number** field. We recommend not using port 80 (the default Web connection port). The default is port 8080.

**4** The current Internet IP address of this device is shown in the **Current IP Address to connect to this device** field.

If the IP address shown is assigned by the ISPs DHCP server, contact the ISP to get a static IP address, or use the DDNS feature (see "Using a dynamic DNS service" on page 43) so you can connect using a domain name rather than an IP address.

To remotely control your router through the Internet, start the browser on the remote computer, type the Internet IP address of the router followed by a colon (:), then type the port number. For example, type http://ip address:port number (assigned in this window). You are prompted for the router's password.

**5** Click **Save** to save your Remote Management entries or **Cancel** to remove your entries. Close the window to return to the *Advanced Features/Configuration* window.
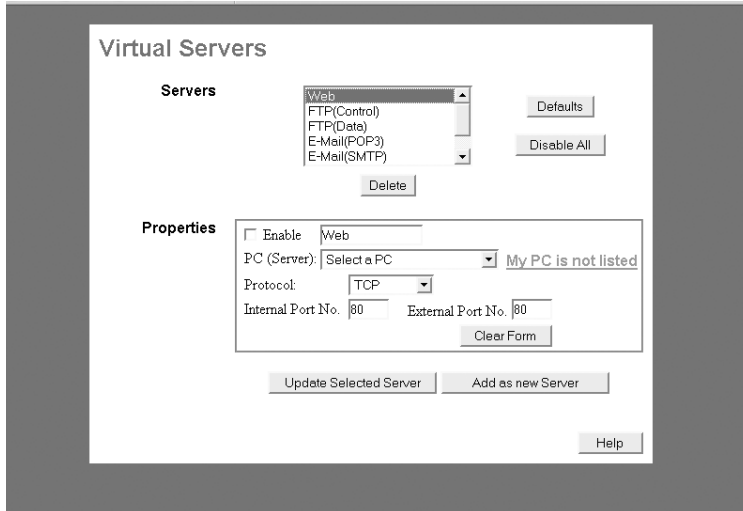
■

# Setting up a virtual server

### To set up a virtual server:

**1** Click **Virtual Servers** in the Advanced Features section. The *Virtual Servers* window opens.



**2** In the Servers section, click the type of server to set up in the **Servers** list. Click **Defaults** to delete servers you have added to the list. Click **Disable All** to disable all virtual servers. To delete a single virtual server, click the server in the list, then click **Delete**.

**3** To enable the selected virtual server, click to select the **Enable** check box in the Properties section, then click the arrow to open the **PC (Server)** list and click the computer you want to act as the server. Default settings for **Internal Port No.** and **External Port No.** are shown for pre-defined servers. If you have made changes to a pre-defined server, click **Update Selected Server** to save the changes.

**4** To configure a new (not pre-defined) virtual server, type the name in the box to the right of **Enable**, then click the arrow to open the **PC (Server)** list and click the computer you want to act as the server. Click the arrow to open the **Protocol** list, then click the type of protocol the server uses. Type the settings for **Internal Port No** (based on the server software) and **External Port No** (normally the same as the Internal Port number). Click **Add as new Server** to add the new server to the Servers list, or **Clear Form** to remove your entries.

**5** Close the window to return to the *Advanced Features/Configuration* window.

# Using a dynamic DNS service

Dynamic DNS is an external service provided by a third party. To set up Dynamic DNS you must register with this third party provider and obtain a user name, a password, and a domain name.

Dynamic DNS lets you use a domain name (which will not change) instead of an Internet IP address (which may change each time you connect to your ISP's server) to connect to your virtual servers.

## To use a Dynamic DNS service:

**1** Click **Dynamic DNS** in the Advanced Features section. The *DDNS (Dynamic DNS)* window opens.



**2** To register for this free service, click the link provided in the *DDNS (Dynamic DNS)* window. After you have registered, use the information provided by the DDNS service to complete the setup process.

**3** Type the information provided by the DDNS service in the **User Name**, **Password**, and **Domain Name** boxes, then click **Save** to save your entries.

**4** Close the DDNS window to return to the *Advanced Features/Configuration* window.

# Upgrading the firmware

New firmware for your router is made available periodically by Gateway. Firmware upgrades may provide enhanced features, increased compatibility, or an updated interface.

Check your firmware version and date (found on the Status page) against the latest version on the Gateway Web site (www.gateway.com). If a new version is available, download it to a computer on your network, then complete the following procedure.

### ▶ To upgrade the firmware:

**1** Click **Upgrade Firmware** in the Advanced Features section. The *Upgrade Firmware* window opens.



**2** Enter the password in the **Wireless Router Password** box.

**3** Click **Browse**, then locate and click the firmware file previously downloaded to your computer, then click **Open** to select the file.

**4** When the upgrade file and path appear in the **Upgrade File** field, click **Start Upgrade** to begin the upgrade process.

**5** When the upgrade process is finished, the router will restart. This may take several minutes and the router's Internet connection will be lost during this time.

**6** Click **Cancel** to remove the information in the **Upgrade File** box. Clicking **Cancel** will not stop the upgrade process if it has already started.

| Important | Do not turn off or reset the router while the firmware is being upgraded. This may cause problems with the router. |

**7** After the firmware upgrade is complete, return to the *Status* window and make sure that the new firmware version and date are shown.

**8** Close the *Upgrade Firmware* window to return to the *Advanced Features/Configuration* window.
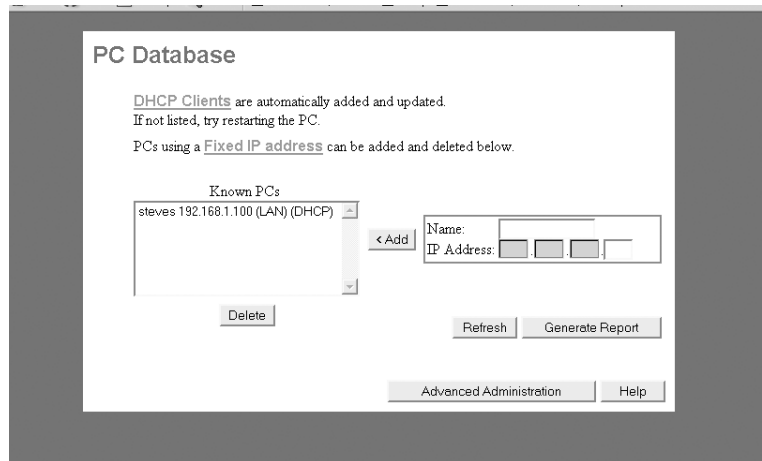
# Using the PC Database

You can use the PC Database whenever you need to select one, several, or all of the computers on your network for a special purpose. This could include setting up virtual servers, DMZ hosting, access control, or many other purposes.

DHCP clients on your network are automatically added to the database. The router always assigns them the same IP address, so there is no need to reserve an IP address. This means that you do not need to assign static IP addresses to computers on your LAN, although you can add static IP addresses to the PC Database if you want.

### To use the PC Database:

**1** Click **PC Database** in the Advanced Configuration section. The *PC Database* window opens.



**2** To add a computer to the PC Database, type the name in the **Name** box and the address in the **IP Address** box, then click **Add**. The computer is added to the **Known PC's** list (and the PC Database).

**3** To see a report listing all of the computers in the PC Database, click **Generate Report**. The report shows the name, IP address, physical (MAC) address, type, and DHCP client status of every computer in the database.

**4** To make detailed changes to the PC Database, click **Advanced Administration**. The *PC Database (Admin)* window opens.



**5** To edit any computer in the database, click a computer in the **Known PC's** list, then click **Edit**. Information about the computer's networking configuration is shown in the *PC Properties* box.

**6** To edit the computer configuration, make changes as required, then click **Update Selected PC**. The PC Database is updated with the new information.

**7** To add a new computer to the PC Database, type the computer name and network configuration information in the *PC Properties* box, then click **Add as New Entry**. The PC Database is updated to reflect the new information.

**8** To clear your entries in the *PC Properties* box without adding them to the PC Database, click **Clear Form**.

**9** To see a report listing all of the computers in the PC Database, click **Generate Report**. The report (see Step 3) shows the name, IP address, physical (MAC) address, type, and DHCP client status of every computer in the database.

**10** Click **Standard Screen** to return to the *PC Database* window.

**11** Close the *PC Database* window to return to the *Advanced Features/Configuration* window.

■

# Changing router options

▶ **To change router Options:**

**1** Click **Options** in the Advanced Configuration section. The *Options* window opens.



**2** In the Backup DNS section, type the backup DNS IP addresses (obtained from your ISP) if the primary DNS is unavailable.

**3** In the TFTP section, click the **Enable Firmware Upgrade using TFTP** check box. If enabled, TFTP (Trivial FTP) can be used to upgrade the router firmware. Instructions for using TFTP are included with the firmware file.

**4** In the UPnP section, click the **Enable UPnP Services** check box. If enabled, new equipment will be automatically detected and configured as it is attached to your LAN. This is only supported by Windows Me, Windows XP and later.

Checking the **Allow Configuration** check box lets you change the configuration of devices that are automatically detected and configured. Leaving it unchecked prevents this.

Checking the **Allow Internet access to be disabled** check box lets you disable Internet access for this device. Leaving it unchecked prevents this.

**5** In the MTU section, type a value for PPPoE and PPTP connections (between 1 and 1500) in the **MTU (Maximum Transmission Unit)** box. This setting should only be changed if advised to do so by Technical Support.

**6** Click **Save** to save your entries, or **Cancel** to remove your entries. Close the window to return to the *Advanced Features/Configuration* window.

# Changing security settings

Network security is important for home networks to protect personal information, such as credit card numbers, Social Security numbers, tax records, and other private information. Network security is vital for business, corporate, or government networks, where the safety of the organization, and possibly the safety of the employees, may be at stake.
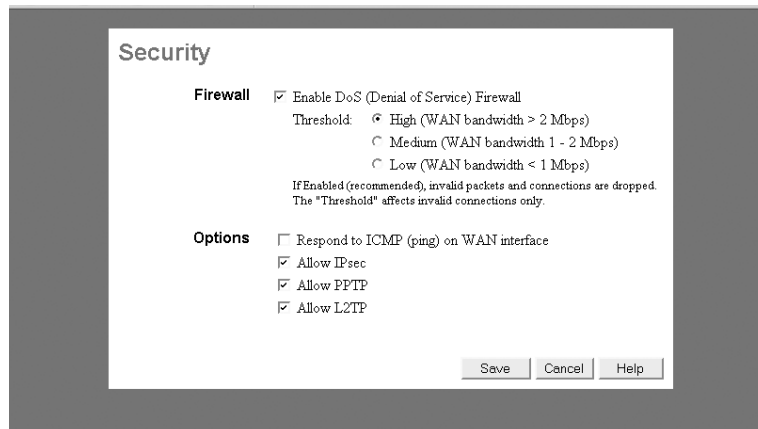
## Establishing a router security scheme

Router security is your first line of defense whenever you are connected to the Internet. Take the time to establish a good router security scheme to prevent unauthorized access to your network.

### To change router security settings:

**1** Click **Security** in the Advanced Configuration section. The *Security* window opens.

**2** In the Firewall section, the **Enable DoS (Denial of Service) Firewall** check box is selected (default). We recommend that you enable this security feature to prevent Denial of Service attacks from overloading your Internet connection and making it unavailable.

Set the Threshold to match the bandwidth of your Internet connection (check with your ISP).

**3** In the Options area, click to select any of the following check boxes:

- **Respond to ICMP (ping) on WAN interface -** If enabled, your router responds to pings from sources on the Internet. Not enabling this option provides a slight increase in security.

- **Allow IPsec -** If enabled, your router allows IPSec connections. IPSec is a protocol used for VPN (Virtual Private Networking) connections to increase security.

- **Allow PPTP -** If enabled, your router allows PPTP (Point to Point Tunneling Protocol) connections. PPTP is a protocol used for VPN (Virtual Private Networking) connections to increase security.

- **Allow L2TP -** If enabled, your router allows L2TP (a security protocol developed by Cisco) connections. L2TP is a protocol used for VPN (Virtual Private Networking) connections to increase security.

**4** Click **Save** to save your entries or **Cancel** to remove your entries. Close the window to return to the *Advanced Features/Configuration* window.

# Change log settings

The *Logs* window lets you request that several logs be kept which record connections, access records, and DoS attacks. You can e-mail the logs to designated recipients at specified intervals.

## ▶ To make log settings:

**1** Click **Logs** in the Advanced Configuration section. The *Logs* window opens.



**2** In the Enable Logs section, click to select any of the check boxes for the logs you want to keep:

- ■ **Outgoing (Internet) connections -** Records all outgoing Internet connections.

- ■ **Access Control -** Records attempted outgoing connections which were blocked by Access Control.

- ■ **DoS (Denial of Service) attacks -** Records the details of all DoS attacks that were blocked by your Firewall.

All logs show the details of the connection or attempted connection. The default on all three of these logs is enabled.

Click the arrow to open the **Timezone** list, then click your time zone so the logs can keep an accurate time record of the log entries.

To view a log, click **View Log** for the log you want.

To restart a log and erase existing log entries, click **Clear Log** for the log you want to reset.

**3** In the E-Mail Reports section, you can elect to have any or all logs e-mailed to a designated recipient at the time specified. Place a check next to the log you want sent, then specify when it will be sent.

**4** In the E-Mail Address section, type the e-mail address of the person you want to receive the e-mailed logs. Also enter the subject of the e-mail and specify the outgoing mail (SMTP) server and port from which the e-mail will be sent.

**5** Click **Save** to save your entries or **Cancel** to remove your entries. Close the window to return to the *Advanced Features/Configuration* window.
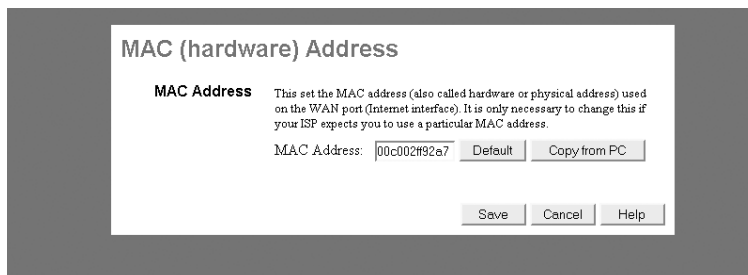
# Set the MAC address

A MAC address is a unique, 12-digit code assigned to networking hardware for identification purposes. Some ISPs require that you provide them with the MAC address of the network interface card that was connected to their DSL or Cable modem during installation. The *MAC Address* window lets you set the MAC address used on the WAN port connection of your router.

### To set the MAC address:

**1** Click **MAC Address** in the Advanced Configuration section. The *MAC Address* window opens.

MAC (hardware) Address

MAC Address    This set the MAC address (also called hardware or physical address) used on the WAN port (Internet interface). It is only necessary to change this if your ISP expects you to use a particular MAC address.

MAC Address:  00c002ff92a7    Default    Copy from PC

Save    Cancel    Help

**2** Type the MAC address of the computer that was initially connect to the DSL or cable modem (the address required by your ISP) in the **MAC Address** box.

- OR -

Click **Copy from PC** to automatically find and copy the MAC address of the computer into the **MAC Address** box. The computer's MAC address appears in the MAC Address field.

**3** Click **Save** to save your entry or **Cancel** to remove your entry. Close the window to return to the *Advanced Features/Configuration* window.

# Configure routing

The *Routing* window lets you configure your router to operate as part of a network with other routers. These settings are only required if there are other routers or gateways on your LAN.

### To set the routing configuration:

**1** Click **Routing** in the Advanced Configuration section. The *Routing* window opens.



In the Static Routing section, the **Static Routing Table Entries** list shows all entries in the Routing Table.
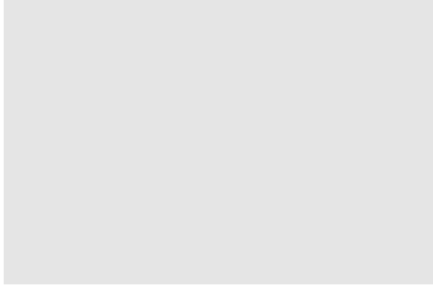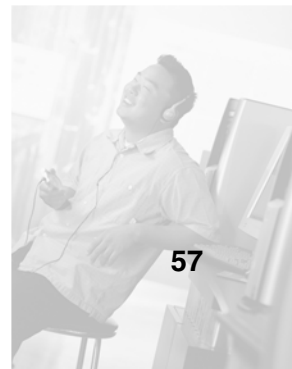
# Troubleshooting

**5**

This chapter provides information on how to resolve common problems experienced with router setup and configuration.

Read this chapter to learn about:

- Ping utility
- Setting a static IP address
- Problem resolution
- Contact information

# Ping utility

You can use the ping utility to help determine whether a connection has been established on a network or to determine a numerical IP address (xxx.xxx.xxx.xxx) based on an alphanumeric Internet or Web address such as www.gateway.com.

Also, your router may have difficulty sending and receiving e-mail or connecting to the Internet if your ISP's mail and server addresses are configured with single words, such as "mail," "home," or "pop3". The router has no way to resolve these abbreviated addresses to the actual IP and Web addresses required for connection. The ping utility can help you find out the required addresses.

### ▶ To use the ping utility to obtain an IP address:

**1** Turn on your computer, the router, and the DSL or cable modem.

**2** Click **Start**, then click **Run**. Type **command** in the **Open** box, then click **OK**.

**3** At the command prompt, type **ping** followed by the single word or verbal address you want resolved (for example "ping mail"), then press **ENTER**.

```
Microsoft(R) Windows DOS
(C)Copyright Microsoft Corp 1990-2001.

C:\DOCUME~2\DEFAULT>ping mail

Pinging mail.adelphia.net [64.8.50.100] with 32 bytes of data:

Reply from 64.8.50.100: bytes=32 time=157ms TTL=53
Reply from 64.8.50.100: bytes=32 time=149ms TTL=53
Reply from 64.8.50.100: bytes=32 time=147ms TTL=53
Reply from 64.8.50.100: bytes=32 time=146ms TTL=53

Ping statistics for 64.8.50.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 146ms, Maximum = 157ms, Average = 149ms

C:\DOCUME~2\DEFAULT>_
```

**4** The ping utility returns the actual IP address of the "mail" server (in this case 64.8.50.100). Write down this number.

This number works as the IP address of your ISP's e-mail server. Unfortunately, this number may change at some point, so it may be necessary to further resolve the number to determine the actual web address of the server. The web address probably will not change.

In the above example, note the line that states "Pinging mail.adelphia.net [64.8.50.100] with 32 bytes of data." In this case "mail.adelphia.net" is the actual Web address of the mail server and does not need to be resolved. Write down this Web address and use it to replace your ISP's one word mail server address (in your Web browser or e-mail program).

However, if the ping utility returned only the IP address, you will need to determine the Web address.

### To resolve an IP address:

**1** With the ping utility still active, type **ping -a 64.8.50.100**, (64.8.50.100 is the IP address returned from pinging "mail"), then press ENTER.

**2** The ping utility returns several lines of information, including one that states "Pinging mail.adelphia.net [64.8.50.100] with 32 bytes of data." In this case "mail.adelphia.net" is the actual Web address of the mail server. Write down this Web address and use it to replace your ISP's one word mail server address (in your Web browser or e-mail program).

# Setting a static IP address

Typically, the computers on your network are set to obtain an IP address dynamically (using the DHCP server function of the router) whenever they contact your local network. However, in certain cases, such as DMZ hosting or port forwarding, you have to assign a static IP address to a computer so that its address remains constant and it can be contacted at the same address over time.

▶ **To set a static IP address using Windows XP:**

1 Click **Start**, then click **Control Panel**. If your Control Panel is in Category View, click **Network and Internet Connections**.

2 Click/Double-click **Network Connections**.

3 Right-click the **Local Area Connection** that is associated with your network adapter card, then click **Properties**.

4 In the **This connection uses the following items** list, click **Internet Protocol (TCP/IP)**, then click **Properties**.

5 In the **IP Address** field, type a unique IP address that will not be used by any other computer on your network. You can use IP addresses between 192.168.1.2 and 192.168.1.99 (IP address 192.168.1.1 is assigned to the router and the router's DHCP server assigns addresses from 192.168.1.100 up to 192.168.1.254).

6 In the **Subnet Mask** field, type **255.255.255.0**.

7 In the **Default Gateway** field, type **192.168.1.1**.

8 At the bottom of the window, click **Use the following DNS server addresses**, then type the **Preferred DNS Server** and **Alternative DNS Server** (contact your ISP if you do not have this information).

9 Click **OK** to close the *Internet Protocol (TCP/IP) Properties* window, then **OK** again to close the *Local Area Connection Properties* window.

### To set a static IP address using Windows 2000:

**1** Click **Start**, **Settings**, then click **Control Panel**.

**2** Double-click **Network and Dial-Up Connections**, right-click the **Local Area Connection** that is associated with your network adapter card, then click t **Properties**.

**3** In the **Components checked are used by this connection** list, click **Internet Protocol (TCP/IP)**, then click **Properties**.

**4** Click **Use the following IP address**.

**5** In the **IP Address** box, type a unique IP address that will not be used by any other computer on your network. You can use IP addresses between 192.168.1.2 and 192.168.1.99 (IP address 192.168.1.1 is assigned to the router and the router's DHCP server assigns addresses from 192.168.1.100 up to 192.168.1.254).

**6** In the **Subnet Mask** box, type **255.255.255.0**.

**7** In the **Default Gateway** box, type **192.168.1.1**.

**8** At the bottom of the window, click **Use the following DNS server addresses**, then type the **Preferred DNS Server** and **Alternative DNS Server** (contact your ISP if you do not have this information).

**9** Click **OK** to close the *Internet Protocol (TCP/IP) Properties* window, then **OK** again to close the *Local Area Connection Properties* window. Restart your computer if asked to do so.

### To set a static IP address using Windows 98SE and Windows Me:

**1** Click **Start**, **Settings**, then click **Control Panel**. The *Control Panel* window opens.

**2** Double click the **Network** icon. The *Network* window opens.

**3** In the **The following network components are installed** list, click the TCP/IP protocol associated with your computer's network adapter (if there is only one TCP/IP protocol, click it), then click **Properties**. The *TCP/IP Properties* window for your network adapter opens.

**4** Select the **IP Address** tab, then click **Specify an IP address**.

**5** In the **IP Address** box, type a unique IP address that will not be used by any other computer on your network. You can use IP addresses between 192.168.1.2 and 192.168.1.99 (IP address 192.168.1.1 is assigned to the router and the router's DHCP server assigns addresses from 192.168.1.100 up to 192.168.1.254).

**6** In the **Subnet Mask** box, type **255.255.255.0**.

**7** Click the **Gateway** tab. In the **New Gateway** box, type **192.168.1.1**, then click **Add**.

**8** Click the **DNS Configuration** tab, then click **Enable DNS**.

**9** Type any Host and Domain name and the DNS IP address provided by your ISP (contact your ISP if you do not have this information).

**10** Click **OK** to close the *TCP/IP Properties* window, then **OK** again to close the *Network* window. Restart your computer if asked to do so.

# Problem resolution

### Your wireless router will not turn on (no LEDs)

- Make sure that the power cord and AC adapter are plugged in and connected to the router.

- Make sure that the power strip, surge protector, or UPS (uninterruptable power supply) is operating correctly.

> **Warning**
>
> Use only the power cord and AC adapter provided with the router. Use of any other power cord or adapter may damage your router and void your warranty

### You have forgotten your password

Press the **Reset** button for about 10 seconds to reset the router to the defaults, then use the default user name and password (admin and admin) to access the Gateway Wireless Router Setup utility. Change the password (see "Establishing a router security scheme" on page 51) and write it down.

### You are having problems connecting to the Internet

1 Turn off the computer, the router and the DSL or cable modem.

2 Turn on the DSL or cable modem and wait several minutes until the modem has established communication with you ISP.

3 Turn on the router, then turn on the computer.

If you still cannot connect, open the Gateway Wireless Router Setup utility and make sure that the settings are all correct (see "Configuring the router" on page 16). You may need to enter additional information, for example your ISP may require a specific MAC address setting on your router (see "Set the MAC address" on page 54).

### You receive a time-out message when you try to enter a URL or address in your browser

- Check the other computers on your network to see if they have the same problem or if the problem is isolated to one specific computer.

- If the problem is isolated:

  - Make sure that the configuration settings are correct (DHCP setting, IP address, subnet mask, default gateway, and DNS), then restart the computer.

- If the problem is general:

  - Make sure that the router is on and configured correctly (see "Configuring the router" on page 16).

  - Make sure that the DSL or cable modem is on and operating correctly (check the LEDs on the front to make sure that it is receiving power and is not on standby).

  - Check with your ISP for outage or cable problems.

  - Try connecting a single computer to the DSL or cable modem to see if connection is possible.

  - If you are connected to a remote server using a VPN, try disconnecting the VPN.

  - Make sure that your browser is set to connect directly to the Internet and not to use a dial-up connection.

## You cannot access your wireless router

- Make sure that your router is turned on (check the power LED).

- Make sure that the SSIDs (wireless) or workgroup name on both the router and the computer are the same (see "Configuring the router" on page 16, and see the documentation that cam with your wireless network card).

- Make sure that the router has the same subnet mask as the computer.

- If you assigned IP addresses to the computers, make sure that all computers have different IP addresses. For home networks, IP addresses should be 192.168.1.N where N is a number you assign between 100 and 254. The N should be different for all computers on your network.

- Press and hold **Reset** button on the back of the router for 10 seconds to reset the router to the default settings.

## You cannot see the other computers on your network

- Make sure that all computers are plugged into a powered electrical outlet and turned on.

- Make sure that all computers on your network have the same workgroup name.

- Make sure that all computers are using the same subnet mask.

- If you are using DHCP though the router, make sure that the other computers are set to obtain IP addresses from DHCP.

- If you assigned IP addresses to the computers, make sure that all computers have different IP addresses. For home networks, IP addresses should be 192.168.N.N where N is a number you assign between 0 and 254. The first N should be the same for all computers on your network and the second N should be different for all computers on your network.

- If you are operating in wireless mode, make sure that the router and each wireless network adapter have the same settings for mode, SSID, channel and encryption type.

- Check the signal strength of your wireless network. For more information, see "Your wireless Ethernet network is running slower than you expect" on page 65.

### Your wireless Ethernet network is running slower than you expect

- If your wireless Ethernet network is running slower than you expect, you should check your network signal strength. If you find the signal strength is low, try moving to a new location to increase the signal strength.

**Important** | Signal strength is affected by the distance between your wireless network devices, by radio interference, and by interference from natural obstructions such as walls, floors, and doors.

### To check the signal strength of your wireless Ethernet network in Windows XP:

1 Click **Start**, then **Control Panel**. The *Control Panel* window opens. If your Control Panel is in Category View, click **Network and Internet Connections**. The *Network and Internet Connections* window opens.

2 Click/Double-click **Network Connections**. The *Network Connections* window opens.

**3** Right-click **Wireless Network Connection**, then click **Status**. The *Wireless Network Connection Status* dialog box opens. The meter shows the signal strength for wireless Ethernet networking on your computer if other computers with the same network name are within range of your computer.
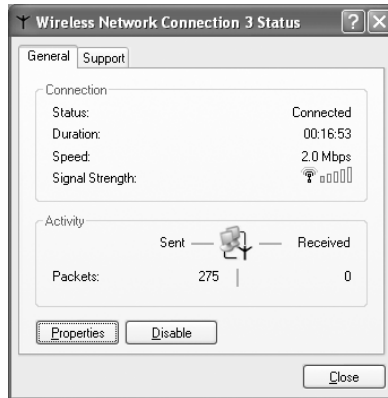
▶ **To check the signal strength of your wireless Ethernet network in Windows 2000, Windows Me, or Windows 98SE:**

**1** Double-click the Gateway Wireless Monitor icon 🖳 on the taskbar. The Gateway Wireless Monitor program opens.



**2** Click the **Available Networks** tab and make sure that you are connected to the network.

**3** Click the **Link Information** tab.

**4** Click **More**. The following screen opens. The meter shows the signal strength for wireless Ethernet networking on your computer if other computers with the same network name are within range of your computer.
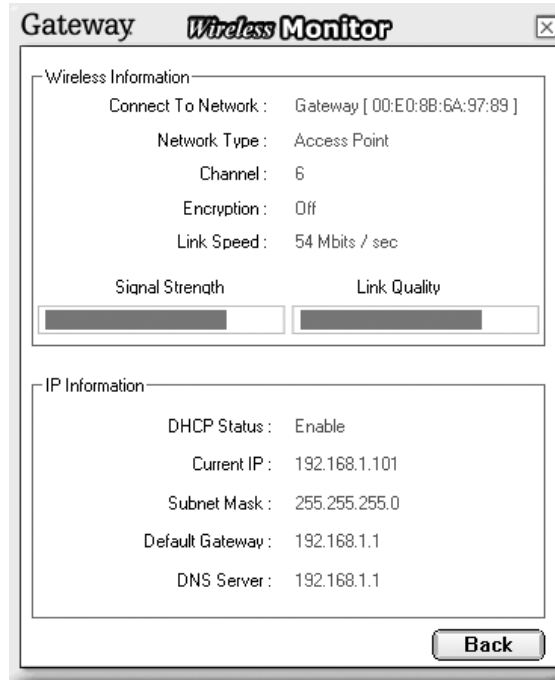
# Technical Support

Gateway offers a wide range of customer service, technical support, and information services.

## Automated troubleshooting system

| Service description | How to reach |
|---|---|
| Use an automated menu system and your telephone keypad to find answers to common problems. | 800-846-2118 (US)<br>877-709-2945 (Canada) |

## Telephone numbers

You can access the following services through your telephone to get answers to your questions:

| Resource | Service description | How to reach |
|---|---|---|
| Fax on demand support | Order a catalog of documents on common problems, then order documents by document numbers. The documents will be faxed to you. | 800-846-4526 (US)<br>877-709-2951 (Canada) |
| Gateway's fee-based software tutorial service | Get tutorial assistance for software issues billed by the minute. | 800-229-1103 (charged to your credit card)<br>900-555-4695 (charged to your telephone bill) |
| Gateway Technical Support | Talk to a Gateway Technical Support representative about a non-tutorial technical support question.)<br>TDD Technical Support (for hearing impaired) is available:<br>Weekdays 6:00 a.m. - 8:00 p.m. Central Time<br>Weekends 6:00 a.m. - 5:00 p.m. Central Time | 800-846-2301 (US)<br>800-846-3609 (Canada and Puerto Rico)<br>605-232-2191<br>(all other countries)<br>800-846-1778 (TDD) |
| Sales, accounting, and warranty | Get information about available systems, pricing, orders, billing statements, warranty service, or other non-technical issues. | 800-846-2000 (US)<br>888-888-2037 (Canada) |

# Glossary **A**

This appendix provides information on terms that relate to routers and networking.
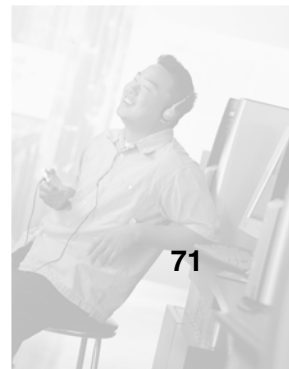
# Terms you should know

**adapter (network)** - A circuit board that plugs into a computer to let the computer connect to a network.

**beacon interval** - A beacon is a periodic broadcast by the router to keep the network synchronized. The interval indicates how often the router broadcasts the beacon.

**broadband** - When multiple signals or channels (such as voice, data, and video) share the bandwidth of a single medium.

**browser** - A program running on a computer which makes it possible to view and interact with the Internet.

**cable modem** - A broadband device that uses a coaxial cable to connect to an ISP to access the Internet.

**CAT 5** - The minimum standard of twisted-pair cable suitable for data transmission over a computer network.

**data packet** - A unit of transmitted data. For more information, see "packet."

**default gateway** - A routing device that forwards data over a local network.

**DHCP (Dynamic Host Configuration Protocol)** - DHCP lets a router or access point router temporarily assign an IP address to a computer on the network.

**DMZ (demilitarized zone)** - DMZ hosting lets a single computer on your LAN expose all of its ports to the Internet. When you set up DMZ hosting on a computer, you bypass the security provided by a router. Consider *port forwarding* as an alternative to DMZ hosting.

**DNS** - A database that translates and stores domain and host names as IP addresses.

**domain** - A set of IP addresses usually "owned" by a company. For example, in an e-mail address the name of the domain comes after the @ symbol.

**DSL (Digital Subscriber Line)** - A broadband Internet connection that uses an ordinary telephone line to provide a fast, "always on" connection to the Internet.

**DTIM (Delivery Traffic Indication Message)** - A message sent by the router to a wireless network device to indicate when the next broadcast or multicast message will be sent. This parameter is necessary to accommodate devices using power save mode.

**dynamic IP address** - An IP address that is temporarily assigned by a DHCP server. Many ISPs use dynamic IP addresses. When a computer connects the Internet, an ISP provides an IP address. When the computer disconnects from the Internet, the ISP reassigns the dynamic IP address to another computer requesting Internet access.

**dynamic routing** - In dynamic routing, a router is configured to automatically generate routing information and share the information with neighboring routers.

**encryption** - The translation of data into a secret code. Encryption is the most effective way to achieve data security. To read an encrypted file, you must have the encryption key (code) associated with the encrypted data. Encryption is especially useful when you are using a wireless network because it prevents outsiders from accessing data. Each computer on a wireless network must use the same encryption code.

**Ethernet** - Ethernet is a common technology used to create computer networks. Wired Ethernet uses cables to link computers, hubs, switches, routers. Wireless Ethernet uses radio waves to create links.

**firmware** - Firmware is programming that is inserted into programmable read-only memory (programmable ROM), thus becoming a permanent part of a computing device. Firmware cannot be modified by a user. Updating firmware requires a special program usually provided by the hardware manufacturer.

**fragmentation** - The process of breaking data into small segments for transmitting. When the segments are received, the data is defragmented and returned to its original format.

**FTP (File Transfer Protocol)** - A simple method of transferring files from one computer to another.

**Gateway** - A system that joins two networks together.

**hardware** - Physical equipment as opposed to software. A router is a hardware device.

**HTTP (HyperText Transport Protocol)** - A system that lets Web browsers and Web servers communicate.

**hub** - A hardware device that joins multiple computers to create a network.

**IP address** - A a number that uniquely identifies a computer on the network.

**IPSec (Internet Protocol Security)** - A standard method for providing data confidentiality, integrity, and the authentication between participating hosts.

**ISP (Internet service provider)** - A company that provides access to the Internet. Most ISPs also provide e-mail addresses.

**LAN (local area network)** - A LAN uses network hardware, such as network adapters, hubs, cables, and wireless devices, to link multiple computers for sharing resources, such files, printers, and an Internet connection.

**MAC (Media Access Control) Address** - A unique number assigned to networking hardware, such as routers, hubs, and network interface cards by the manufacturer.

**Mbps (MegaBits Per Second)** - Transfer speed of 1 million bits per second.

**network** - Two or more computers linked together for the purpose of sharing resources, such as files, printers, or a Internet connection. Routers are often used to link the device, especially if the network includes more than two computers.

**packet** - A unit of transmitted data. When a server sends information, such as e-mail messages and files, through the Internet, the server divides the information into *packets* that contains identifying information called *headers* and *footers*. The system receiving the information uses the headers and footers to reassemble the information.

**passphrase** - Similar to a password, a passphrase is a sequence of characters used by the router to create encryption keys.

**ping (Packet INternet Groper)** - A network utility that determines if a remote device, such as a server, can be reached on the network. For more information, see "Ping utility" on page 58.

**plug-and-play** - If a device is a *plug-and-play* device, a computer can automatically detect and configure the device and install the appropriate software called a device driver.

**port** - A computer program using TCP/IP sends information to another computer through a *port*. Ports are assigned numbers that come after a standard IP address. Many programs hide these port numbers to reduce the complexity of TCP/IP.

**port forwarding** - Port forwarding, unlike DMZ hosting, lets a single computer on your LAN expose only one of its ports to the Internet. This type of port exposure has more security than DMZ hosting.

**PPPoE (Point to Point Protocol over Ethernet)** - A communications protocol that combines the Ethernet and Point-to-Point Protocol (PPP) standards. PPPoE is sometimes used with broadband modems.

**PPTP (Point-to-Point Tunneling Protocol)** - A protocol that lets a private network connect securely to another private network through private "tunnels" over the public Internet. This kind of interconnection is known as a virtual private network (VPN).

**protocol** - A set of communication rules. When two computers or networks use the same protocol, they can communicate with each other.

**RIP (Routing Information Protocol)** - A protocol used by a router to maintain routing tables of configuration information to filter incoming and outgoing traffic based on the IP addresses of the senders and receivers.

**RJ-45** - RJ-45 jacks connect a computer to a router. In a wired network, one end of a network cable is plugged into the RJ45 jack on a computer. The other end of the cable is plugged into an RJ45 jack on a router. Data is passed to and from the computer and router through the RJ45 jacks.

**router** - A hardware device that connects devices in a network. A router can also provide Internet access to the networked devices.

**RTS (Request To Send)** - A signal sent by a receiving device, like a router, that tells the sending device to begin transmission.

**server** - A computer that provides shared network service to a network. For example, a server can provide file and printer sharing between networked computers.

**SSID (Service Set IDentifier)** - In a wireless network, the SSID identifies a network. All computer in the network must use the same SSID.

**static IP address** - An IP address that is permanently assigned to a device.

**static routing** - The routing of network information through a single, set path.

**subnet mask** - This number identifies what subnetwork the computer is located on. This number is the same on all computers on a home network.

**switch** - Like a hub, a switch is a hardware device that links computers to create a network. A switch provides better data routing than a hub.

**TCP (Transmission Control Protocol)** - A protocol used in connection with Internet Protocol (IP) to let computers communicate over the Internet.

**TCP/IP** (Transmission Control Protocol/Internet Protocol) - A combination of two protocols (TCP and IP) that lets computers communicate with Web servers.

**UDP (User Datagram Protocol)** - UDP is a simpler, faster protocol than TCP. UDP is used with IP. Unlike TCP, UDP drops packets without retries and packets are received in a different order than they were sent. UDP is often used in videoconferencing applications or games where speed is preferred over guaranteed message delivery.

**upgrade** - An addition or update to a program that provides additional features or "fixes."

**URL (Uniform Resource Locator)** - A standard method of specifying a Web location, for example the URL for Gateway is www.gateway.com. Also called a *Web address*.

**VPN (Virtual Private Network)** - A private network link that lets a computer communicate with another network over the Internet. VPNs usually use encryption to provide secure communication.

**WAN (Wide Area Network)** - A network that provides data communications to a large number of independent users spread over a large geographic area. A WAN often links several networks. The Internet is a WAN.

**WEP (Wired Equivalent Privacy)** - A protocol that adds security to wireless local area networks (WLANs). WEP uses encryption to provide security.

# Specifications

# B

This appendix provides information on your router specifications.
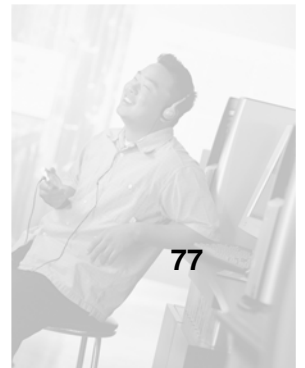
# Specifications

Specifications are subject to change without notice or obligation.

| | |
|---|---|
| **Dimensions** | 7.32 × 6.89 × 1.89 ins. (186 x 175 x 48 mm) |
| **Weight** | 17 oz. (0.482 Kg) |
| **Color** | Graphite and Platinum |
| **Power consumption** | 50 mW to 200 mW |
| **Power supply** | Input 120V AC Output 12V DC |
| **Operating temperature** | 0° to 40° C (32° to 104° F) |
| **Operating humidity** | 10% to 85% non-condensing |
| **Non-operating temperature** | -20° to 70° C (-4° to 158° F) |
| **Non-operating humidity** | 5% to 90% con-condensing |
| **MTBF** | 500,000 hours |
| **Operating range (indoors)** | As much as 70 m (230 ft) @ 11 Mbps |
| | As much as 91 m (300 ft) @ 6 Mbps |
| **Certifications** | FCC Part 15 Class B Report (Subpart C) |
| | FCC part 15 Class B DoC (Declaration of Conformity) |
| | UL |
| | CAS or CUL |

# Safety, Regulatory, and Legal Information

# C

## Regulatory compliance statements

### Wireless Guidance

The WBR-100 802.11b wireless LAN, (low power Radio Frequency, RF, transmitting device), operates in the 2400 - 2483.5 MHz band. The following section is a general overview of considerations while operating the wireless LAN.

Limitations, cautions, and concerns are listed below and in the specific country sections (or country group sections). This wireless device is only qualified for use in the countries identified by the Radio Approval Marks on the device rating label. If the country you will be using the wireless device in is not listed, please contact that countries local Radio Approval agency for requirements prior to operation. Wireless devices are closely regulated and use may not be allowed.

The power output of the WBR-100 wireless LAN device is well below the RF exposure limits as known at this time. Because this wireless device emits less energy than is allowed in radio frequency safety standards and

recommendations, Gateway believes these devices are safe for use. Regardless of the power levels, care should be taken to minimize human contact during normal operation.

Measurements have been performed to show that the RF exposure is below what is considered safe limits; however care should be taken to make sure the user or bystanders keep the transmitter away from their body when the wireless device is transmitting. The transmitting antenna should be installed and used in a manner to maintain 20cm (8 inches) from user's or bystander's bodies.

This wireless device is intended to be used indoors. In some areas, use of this device outdoors is prohibited.

Some circumstances require restrictions on using wireless devices. Examples of common restrictions are listed below:

| **Warning** | High voltages can enter your computer through both the power cord and the modem connection. Protect your computer by using a surge protector. If you have a telephone modem, use a surge protector that has a modem jack. If you have a cable modem, use a surge protector that has an antenna/cable TV jack. During an electrical storm, unplug both the surge protector and the modem. |
|---|---|
| **Warning** | In environments where the risk of interference to other devices or services is harmful or perceived as harmful, the option to use a wireless device may be restricted or eliminated. Airports, Hospitals, and Oxygen or flammable gas laden atmospheres are limited examples where use of wireless devices may be restricted or eliminated. When in environments where you are uncertain of the sanction to use wireless devices, ask the applicable authority for authorization prior to use or turning on the wireless device. |
| **Warning** | Every country has different restrictions on the use of wireless devices. Since your system is equipped with a wireless device, when traveling between countries with your system, check with the local Radio Approval authorities prior to any move or trip for any restrictions on the use of a wireless device in the destination country. |
| **Warning** | Do not operate the wireless device unless all covers and shields are in place and the system is fully assembled. |
| **Warning** | Wireless devices are not user serviceable. Do not modify them in any way. Modification to a wireless device will void the authorization to use it. Please contact Gateway for service. |

| **Warning** | Only use drivers approved for the country in which the device will be used. See the Gateway System Restoration Kit, or contact Gateway Technical Support for additional information. |

| **Warning** | In order to comply with FCC requirements this transmitter must not be operated (or co-located) in conjunction with any other transmitter or antenna. |

# United States of America

**Federal Communications Commission (FCC)**
**Intentional emitter per FCC Part 15**

The power output of the WBR -100 wireless LAN device is well below the RF exposure limits as known at this time. Because this wireless device emits less energy than is allowed in radio frequency safety standards and recommendations, Gateway believes these devices are safe for use. Regardless of the power levels, care should be taken to minimize human contact during normal operation.

Measurements have been performed to show that the RF exposure is below what is considered safe limits; however care should be taken to make sure the user or bystanders keep the transmitter away from their body when the wireless device is transmitting. The transmitting antenna should be installed and used in a manner to maintain 20cm (8 inches) from user's or bystander's bodies.

This wireless device is intended to be used indoors. In some areas, use of this device outdoors is prohibited.

Operation of this device is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation of the device.

| **Warning** | Wireless devices are not user serviceable. Do not modify them in any way. Modification to a wireless device will void the authorization to use it. Please contact Gateway for service. |

**Unintentional emitter per FCC Part 15**

This device has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio or television reception. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause

interference to radio and television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna
- Increase the separation between the equipment and receiver
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected
- Consult the dealer or an experienced radio/TV technician for help.

**Compliance Accessories**: These accessories are required to be used in order to ensure compliance with FCC rules: The AC Adapter that came with the router.

**FCC declaration of conformity**

Responsible party:

Gateway Companies, Inc.
610 Gateway Drive, North Sioux City, SD 57049
(605) 232-2000   Fax: (605) 232-2023

Product:

▪ Gateway WBR-100

This device complies with Part 15 of the FCC Rules. Operation of this product is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

| **Warning** | Changes or modifications not expressly approved by Gateway could void the FCC compliance and negate your authority to operate the product. |
|:---:|:---|

# California Proposition 65 Warning

| **Warning** | This product contains chemicals, including lead, known to the State of California to cause cancer and/or birth defects or reproductive harm. |
|:---:|:---|

# Notices

MAN 802.11B ROUTER GDE R0  8/03

8509439